4. How do you configure Nessus for optimal performance?

🔥 Optimizing Nessus for Maximum Performance 🔥

To ensure **Nessus runs efficiently**, you need to **optimize scanning speed, accuracy, and resource usage**. Below are key **best practices** for configuring Nessus to deliver fast and accurate results while minimizing false positives.

🔹 1. Optimize Performance Settings in Nessus

🛠️ Step 1: Adjust Global Scan Settings

1️⃣ **Log into Nessus Web Interface** → `https://localhost:8834`
2️⃣ Go to **"Settings" > "Advanced Settings"**
3️⃣ Modify the following parameters:

Setting	Default	Optimized Value	Purpose
`Max simultaneous hosts`	5	10-15 (depends on CPU/RAM)	Number of hosts scanned in parallel
`Max simultaneous checks per host`	4	8-12	Number of vulnerability tests per host
`Network Receive Buffer Size`	0	524288	Improves network scan efficiency
`Global Max Hosts Per Scan`	100	Adjust based on system power	Controls large scans to prevent overload

---

🔹 2. Optimize Scan Policies for Faster & More Accurate Results

🛠️ Step 1: Create a Custom Scan Policy

1️⃣ Go to **"Scans" > "Policies"**
2️⃣ Click **"New Policy"**
3️⃣ Adjust the settings:

✅ **Reduce False Positives:**

- Enable **"Safe Checks"**
- Use **"Authenticated Scanning"** for more accuracy

✅ **Prioritize Critical Vulnerabilities:**

- Select **CVSS ≥ 7** to focus on high-risk issues
- Use **"CVE Only"** if you're tracking known exploits

✅ **Enable Performance Features:**

- **Concurrent TCP Sessions:** Increase to **25-50** for faster scanning
- Enable **"Avoid Sequential Scanning of IPs"** to reduce scan time

---

🔹 3. Enable Credentialed Scanning for Deeper Insights

Why? Authenticated scans allow Nessus to check **inside** the system instead of just relying on open ports.

🛠️ How to Add Credentials:

1️⃣ Go to **"Scans" > "New Scan"**
2️⃣ Choose **"Credentialed Scan"**
3️⃣ Under **"Credentials"**, add:

- **Windows:** Local Admin credentials
- **Linux:** SSH keys or root password
- **Cloud (AWS, Azure, GCP):** API keys for cloud asset scanning

✅ **Benefits of Credentialed Scanning:**
✓ Detects hidden vulnerabilities
✓ Reduces false positives
✓ Provides in-depth security analysis

🔹 4. Optimize Resource Usage (CPU/RAM Considerations)

If Nessus slows down your system, tweak these settings:

✅ **Increase RAM & CPU Allocation:**

- **Linux:** Edit `/opt/nessus/etc/nessus/nessusd.conf`

```
max_hosts = 10
max_checks = 8
```

- **Windows:** Use `Task Manager > Set Process Priority to High`

✅ **Schedule Scans During Off-Peak Hours:**

- Go to **"Scans" > "Schedule"** and set scans for **midnight or non-business hours**

✅ **Disable Unused Plugins:**

- Go to **"Scans" > "Plugins"**
- Disable unnecessary categories like **SCADA, VoIP, or Web Applications** (if not needed)

🔹 5. Use Network Segmentation to Speed Up Large Scans

Instead of scanning your **entire network at once**, **break it into segments**:

🚀 **Example:**

- `192.168.1.0/24` → High-priority assets
- `192.168.2.0/24` → Non-critical assets
- `10.10.0.0/16` → External network scan

✅ **Create Separate Scan Policies for Each Subnet** to avoid resource exhaustion

---

🔹 6. Automate Scans & Reporting

🛠️ How to Automate Nessus Scans

1️⃣ Go to **"Scans" > "New Scan"**
2️⃣ Choose **"Basic Network Scan"**
3️⃣ Click **"Schedule"**
4️⃣ Set scans to run **weekly/daily** based on risk level

✅ **Enable Auto-Report Generation:**

- Under **"Reports"**, enable **"Export to CSV/PDF"**
- Send reports via **email or API integration**

🎯 Final Tips for Nessus Performance Optimization

✓ **Use Credentialed Scans** → Avoid false positives & improve accuracy
✓ **Increase Parallel Host/Check Limits** → Faster scans without losing detail
✓ **Run Scans at Off-Peak Hours** → Avoid network congestion
✓ **Tune Nessus Plugin Selection** → Only enable what you need
✓ **Segment Networks & Schedule Smartly** → Scan priority assets first